

APPLICATION UNDER UNITED STATES PATENT LAWS

Invention: **ENCRYPTION OF VOICE AND DATA IN A SINGLE DATA STREAM
IN A DEPLOYABLE, SECURE COMMUNICATION SYSTEM**

Inventor(s):
Steve ANSPACH

Manelli Denison & Selter PLLC
2000 M Street, NW
7th Floor
Washington, DC 20036-3307
Attorneys
Telephone: (202) 261-1000

This is a:

- Provisional Application
- Regular Utility Application
- Continuing Application
- PCT National Phase Application
- Design Application
- Reissue Application
- Plant Application

SPECIFICATION

ENCRYPTION OF VOICE AND DATA IN A SINGLE DATA STREAM IN A DEPLOYABLE, SECURE COMMUNICATION SYSTEM

The present application claims priority from U.S. Provisional
5 Application No. 60/502,660, entitled "Encryption of Voice and Data in a
Single Data Stream in a Deployable, Secure Communication System",
filed September 15, 2003.

BACKGROUND OF THE INVENTION

10 1. Field of the Invention

This invention relates generally to computer and communication networks, and more specifically, to handling of encrypted data in a deployable communication system used to provide secure voice, video and data services to multiple remote users.

15

2. Background of Related Art

Fig. 5 is a depiction of a conventional deployable secure communication system providing voice communications.

In particular, as shown in Fig. 5, a secure encryption module such as defined by KIV-7 standards 912 with suitable interface hardware is utilized in a direct connection path between a remote user 910 and a wireless connection to a similarly secure receiver via a satellite antenna 914. In the conventional system of Fig. 5, a conventional ISDN phone 910 is at the remote user end, and an ISDN link is utilized between the KIV-7 encryption module 912, and a suitable satellite two-way communication transceiver and antenna 914.

In operation, voice data is generated by a suitable ISDN telephone 910, and is encrypted by the Type 1 encryption unit 912. The encryption unit 912 has a serial data output, e.g., a synchronous serial output such as is defined by RS-530 standards.

The serial data passed from the encryption unit 912 is converted into an ISDN data stream by a suitable serial-to-ISDN converter 917, and transmitted in a secure environment over a physically secure satellite, e.g., an M4 INMARSAT satellite terminal.

5 The conventional communications terminal shown in Fig. 5 provides voice communications from a single ISDN phone 910. The ISDN standard allows up to two voice channels, together with a small control data channel. However, there are growing needs for computer data (e.g., from a laptop computer) to be communicated from a remote, deployable, 10 secure communications terminal through a secure, encrypted means.

Fig. 6 is a depiction of a conventional deployable secure communication system allowing both voice and data communications.

15 In particular, as shown in Fig. 6, a voice data path is provided by an ISDN telephone 910, which generates a serial data stream that is encrypted through a Type 1 encryption unit 912a, e.g., a KIV-7 encryption unit. Additionally, an Ethernet 10BaseT serial data stream is generated by a laptop computer 111, and encrypted by a similar Type 1 encryption unit, e.g., another KIV-7 encryption unit 912b. The two encrypted serial data streams from the KIV-7 units 912a, 912b are then 20 multiplexed together, converted back into a suitable post-encryption ISDN data stream by a serial to ISDN converter 917, and passed on to the Inmarsat satellite terminal 914 for transmission to a satellite network.

25 It is vitally important that encryption units 912 stay physically secured, to maximize protection of the information being passed thereover. Also, to further maximize protection of the information, the satellite terminal 914 is conventionally set up and maintained within a secure environment, and travels with the secure encryption module.

30 It is also vitally important that secure communications terminals, particularly those communication terminals that are intended to be deployed in a military environment, be as small as possible. Conventional systems are typically physically large, e.g., the size of a van,

due in significant part to the need for two separate Type 1 encryption units **912a, 912b** in a secure, deployable communications terminal to handle two serial data streams providing both voice and data support.

5 There is always a need for a smaller, more lightweight, more easily portable and more easily deployable communication system.

BRIEF DESCRIPTION OF THE DRAWINGS

10 Features and advantages of the present invention will become apparent to those skilled in the art from the following description with reference to the drawings, in which:

Fig. 1 is a block diagram of an exemplary deployable secure communication system, in accordance with a first embodiment of the present invention.

15 Fig. 2 is a more detailed block diagram of the exemplary deployable secure communication system shown in Fig. 1.

Fig. 3 shows encrypted data encapsulated within an IP packet, in accordance with the principles of the present invention.

20 Fig. 4 shows that the encrypted data encapsulated within an IP packet may be Voice over IP data (VoIP).

Fig. 5 is a depiction of a particular conventional deployable secure communication system.

Fig. 6 is a depiction of a conventional deployable secure communication system allowing both voice and data communications.

25

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, a method and apparatus for encrypting and transmitting voice and data together in a secure communication system comprises packetizing voice data into a voice-over-IP (VoIP) data stream. The VoIP data stream is encrypted through a Type 1 encryption unit into an encrypted data stream.

The encrypted data stream is encapsulated into IP packets for transmission.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

5 In accordance with the principles of the present invention, separate IP data streams, including both voice (VoIP) and data sources, are routed over a single network data stream, encrypted by a single KIV encryption unit, and transmitted as a single packet data stream including both computer and voice data. Integration of the use of a VoIP data
10 stream, together with data sources, and encrypted through a single serial encryption unit such as a KIV-7 enables the encryption of both voice and data using a single KIV encryption unit. After encryption by the Type 1 encryption unit (e.g., KIV-7) in a remotely deployed, secure communication system, the single encrypted data stream is encapsulated
15 into IP packets. The IP packets are addressed to a distant IP device that removes the encapsulated, encrypted data and passes it to a similar Type 1 KIV device for decryption, and distributed to voice devices and computer devices via another voice-enabled router.

20 Conventional voice and data Type 1 encryption communication systems had required the use of at least two KIV encryption units-one for a voice data stream as well as another for a data serial stream. Thus, only one Type 1 encryption unit is required, saving the enormous cost associated with the use of a second Type 1 encryption unit.

25 After encryption by the Type 1 encryption unit (e.g., KIV-7) in a remotely deployed, secure communication system, the single encrypted data stream is encapsulated into IP packets. The IP packets are addressed to a distant IP device that removes the encapsulated, encrypted data and passes it to a similar Type 1 KIV device for
30 decryption, and distributed to voice devices and computer devices via another voice-enabled router. The IP encapsulated, encrypted data may

be passed over the public Internet, taking advantage of the wide availability and flexibility of the Internet.

In this way, encrypted data need not be maintained within a totally secure network transmission system, because it doesn't look like 5 government encrypted data (i.e., it doesn't look like a KIV signal). Rather, the encrypted data, being encapsulated in IP packets, looks just like any other commercial IP transmission from just about any other IP device. Thus, sensitive, encrypted data is made to appear as if it were any other commercial network data.

10 The present invention is embodied in a system that provides secure Voice-Over-IP (VOIP), video and data network functionality in a single, small size deployable case, to a remote user. While capable of secure communications, the disclosed system also provides communication capability (VOIP, video and/or data) in a non-secure 15 manner if desired. Most importantly, the embodiment allows for the routing of bulk encrypted (i.e., secure) data over a public network, e.g., the Internet.

The disclosed deployable secure communications system can be deployed even at the most remote regions of the world where no 20 other communication means are available, taking advantage of the satellite direct connection link, or (very importantly) in more developed regions that might include access to the Internet (e.g., in a hotel room, high speedx).

The disclosed deployable secure communications system 25 can be deployed to provide a multitude of applications for remote users. Uses include emergency response, news reporting, public safety, drilling and mining operations, field surveys and other activities that require remote capabilities for video and data transmissions.

The system, once deployed and operational, offers access 30 to the Internet or corporate network using a direct link via an Inmarsat M4 GAN network or ISDN terrestrial circuit. For those systems configured

with a KIV-7 encryption device, access to the SIPRNET and other secure voice and data networks is possible. However, importantly, the disclosed deployable secure communication system also provides an access point for a direct link to a local enterprise network providing IP encapsulated information for transmission over a network such as the Internet. In this way, bulk encrypted data may be routed using an available link (e.g., a wired Ethernet port in a hotel room, high speed cable, etc.) Thus, secure data communications and/or voice-over-IP communications over the Internet are possible.

10 The disclosed deployable communication system provides a single user, or multiple users, remote secure access to a local enterprise network, and thus access to services conventionally provided only to direct connected users. Also, up to two simultaneous voice over IP calls may be established along with normal data connectivity via, e.g., a laptop computer.

15 Fig. 1 is a block diagram of an exemplary deployable secure communication system, in accordance with a first embodiment of the present invention.

20 In particular, Fig. 1 shows a deployable communications module **112** including a secure encryption module **100**, e.g., one built according to KIV-7 requirements, a voice enabled router **202**, and an IP encapsulator of serial data **204**. On the red, non-secure side of the deployable communications module **112**, a voice-enabled router **202** combines voice communications **110** from a suitable digital telephone such as an ISDN telephone together with data communications from one or more computers **111** or other digital device are provided with suitable interfaces.

25 The IP encapsulator **204** is a full-duplex device providing both IP encapsulation of encrypted synchronous serial RS-530 data emanating from the encryption unit **200**, as well as IP decapsulation of IP data addressed to the IP address of the IP encapsulator **204** from a

distant source, and passing the decapsulated, presumably encrypted data to the RS-530 synchronous serial data port of the encryption unit 200 for playback by the telephone 110 (if voice data) or receipt by the laptop computer 111 (if data destined for the computer).

5 The digital telephone 110 may be, e.g., an ISDN type utilizing a digital subscriber link to the voice enabled router 202 of the deployable communications module 112. The laptop computer 111 may communicate with the deployable communications module 112 using a standard Ethernet 10baseT or 100baseT type network link.

10 On the black, or secure side, the disclosed deployable system includes an Inmarsat M4 terminal 114 providing a direct connection to an enterprise network via a satellite. The M4 Satellite terminal is, e.g., a Nera WorldCommunicator portable Inmarsat M4 satellite terminal, which is a portable Inmarsat M4 satellite terminal 15 capable of providing 64kbps ISDN connectivity to remote users. Additional features include a 3-panel antenna with RF transceiver; a wireless DECT 2.4Ghz Handset; and a modem unit and battery pack.

20 The embodiment also provides an Ethernet direct connection to a local enterprise network, e.g., a hotel Ethernet network having direct access to the Internet, high speed cable, etc. Thus, when the deployable communication system is in the convenience of modern accommodations, such as in a hotel or other public place that provides an Ethernet link to the Internet, such services may be utilized without the need to set up the direct connection using the Inmarsat M4 terminal 114.

25 It is important to understand that this direct connection to the Internet is on the black side of the deployable communication system, thus bulk encrypted data (i.e., secure data) may be conveniently routed along the public Internet 101 to a desired destination. This saves bandwidth on the relevant satellite, and also battery power necessary to 30 drive the satellite transceiver. It also simply provides secure

communications while in a hotel room or similar public place, near a cable modem, etc.

Fig. 2 is a more detailed block diagram of the exemplary deployable secure communication system shown in Fig. 1.

5 In particular, as shown in Fig. 2, the deployable communications module 112 includes a black (encrypted, or secure) portion and a red (non-encrypted, or unsecure) portion.

10 The red portion includes the voice enabled router 202. In the disclosed embodiments, a commercially-available CISCO™ Model Number 1751-V voice enabled Modular Access Router was utilized. Of course, other brands and types of voice enabled routers are equally applicable to the present invention.

15 The voice-enabled router 202 in the disclosed embodiment is provisioned with one fast Ethernet (10/100BaseTX) port as well as interface cards to support either WIC or VIC modules. The fast Ethernet port interfaces with an Ethernet network 113 including the shown laptop computer 111 as well as other data devices communicating over the Ethernet network 113.

20 Moreover, and importantly, the voice enabled router 202 is provisioned to support a voice-over-IP connection. The CISCO 1751-V voice enabled router is commercially available with features allowing integration of data and voice services with support for up to two voice channels (32 MB Flash and 96 MB DRAM, one DSP (PVDM-256K-4), and a Cisco IOS IP Plus Voice feature set). Voice and WAN interface cards 25 are added, allowing interfacing to analog telephones and an Ethernet, respectively.

30 The particular router 202 chosen for integration in the disclosed deployable, secure communication system, the CISCO™ 1751-V, includes three modular slots for voice and data interface cards, an autosensing 10/100BaseT Fast Ethernet LAN port supporting standards-based IEEE 802.1Q VLAN, a console port, and an auxiliary port. A

suitable data interface card is a WAN interface card, and a suitable voice interface card is a voice-over-IP (VoIP) card.

A WAN interface card may be installed in the voice-enabled router 202 to enable any of a wide range of data services, including 5 synchronous and asynchronous serial, Integrated Services Digital Network Basic Rate Interface (ISDN BRI), ADSL, and serial with DSU/CSU options for primary and backup WAN connectivity. Thus, data to be encrypted and transmitted by the secure, deployable communication terminal may be sourced from any of many different types of networks 10 and/or data devices. Alternatively, an Ethernet interface card may be installed in the voice-enabled router 202 to provide dual-Ethernet capability to support broadband modem devices.

Moreover, commercially available voice interface cards for the voice-enabled router 202 support Foreign Exchange Office (FXO), 15 Foreign Exchange Station (FXS), Network and User Side Voice BRI (ISDN BRI NT/TE), Ear & Mouth (E&M), direct inward dial (DID), and T1/E1 Multiflex VWICs. Thus, while an ISDN telephone 110 is shown, an analog or other type voice telephone, analog or digital, is equally applicable for use with the present invention.

20 The red portion also includes a suitable power supply such as the +5V, +12V and -12V power supply 212 shown in Fig. 2. The red components are shielded in a suitable RFI/EMI shielding preferably providing -40dB to -60dB of isolation. The compartment in which the red components sit may also be coated with a suitable RFI/EMI isolating 25 coating.

The black portion includes a KIV-7 device 200 such as the KIV-7HSB shown in Fig. 2. The disclosed KIV-7HSB is a Mykotronx KIV-7 module is a standard compact, economical, high performance, and user-friendly COMSEC device, designed to meet users' needs for secure data 30 communication links. Features of this unit include Commercial Off-the-shelf (COTS) Type I data encryption; KG-84/-84A/-84C interoperability;

User-friendly menu-based operator interface; and Standard D-type rear-panel interface connectors.

The IP encapsulator 204 may be any suitable product that can invisibly encapsulate serial data (e.g., synchronous serial data from an RS-530 port) into IP packets addressed to another IP encapsulator 5 204 operating to de-encapsulate the same IP packets and pass the data back into a suitable serial data stream (e.g., an RS-530 data stream). Thus, the IP encapsulator 204, IP network, and receiving IP encapsulator operate invisibly as if the RS-530 data ports (sending and receiving) were 10 plugged into one another. The product utilized in the disclosed embodiment is an IPTube-RS530 model that is commercially available from Engage Communication in Aptos, California.

The IP encapsulator 204 encapsulates encrypted data, and passes it either to an Ethernet port which may be wired directly to an 15 Ethernet network having access to the Internet 101, or to a black-side router 206 (e.g., commercially available from CISCO). The router 206 includes an ISDN port (ISDN/BRI/ST) to link to the Inmarsat M4 terminal 114.

The KIV-7 preferably uses a serial RS-530 connection both 20 on its red side to the red side router 202, as well as on the black side to connect to the IP encapsulator 204. The red side router 202 is suitably configured for operation with the KIV-7 encryption device 200.

The red side router 202 is configured to allow for transparent, automated operation for the user. All off-network traffic is 25 routed via the serial port to the KIV-7HSB for bulk encryption. In addition, the voice ports are configured so that dialing a "9" (or any other string desired by the user) will result in off-network traffic and be routed to the distant end gateway.

The particularly IP encapsulator 204 used in the disclosed 30 embodiments, the IPTube, allows acceptance of encrypted data. The clock in the IPTube is preferably tuned to match the RS-530 synchronous

serial data output of the KIV-7HSB. In addition, it is further preferred that the IPTube allow for a dial-on-demand type feature so that the IP encapsulator 204 would be in an idle state until interesting traffic were presented.

5 The IP encapsulator 204 is configured so as to seek a specific distant end device and establish a dedicated tunnel therewith. The internal side of the IP encapsulator 204 is configured to seek a specific (distant end) IP address. The distant end device is configured to seek the opposite. Once located, the two IP encapsulators 204
10 communicate and establish the tunnel.

Fig. 3 depicts an IP packet encapsulating a payload of encrypted data 302 encrypted by an encryption unit such as the KIV-7. The IP packet 300 is addressed to another IP encapsulator also accessible to the relevant IP network, e.g., the Internet. The receiving IP
15 encapsulator retrieves the encrypted data 302 from the IP packet, and converts it back to the appropriate serial data form (e.g., synchronous RS-530 data), and passes it on to its encryption unit (e.g., a KIV-7) for decryption.

Fig. 4 shows that the encapsulated encrypted data may be
20 Voice over IP data (VoIP).

Referring back to Fig. 2, the laptop computer 111a depicts in solid line a one-to-one connection into the red side router 202. In a dotted line depiction, multiple computing devices 111a-111b may be networked over a conventional Ethernet network 111c, with the red side router 202
25 being a member of that Ethernet network 111c.

Any computing device capable of an Ethernet connection may be implemented. In the disclosed embodiment, the laptop computers that were implemented were Panasonic Toughbooks™. Those laptop computers are ruggedized in that it is shock, dust, vibration and water
30 resistant, making it a good choice for a deployable communication

system. Additional features include design to MIL-STD-810F test procedures; and password security (Supervisor, User), "Access Key".

The deployable communication system communicates over the Internet (considered black with respect to the bulk encrypted data 5 passed through the Ethernet port of the IP encapsulator 204) with a suitable IP gateway (not shown). As long as both sides know the IP address of the other, and the IP encapsulator 204 is properly configured, communications will be enabled.

Both the red side router 202 and the black side router 206 10 are configured to maintain QOS. The link fragmentation and packet interleaving are preferably implemented to assure voice quality. PPP multilinking may be utilized to maximize performance.

Routing information is not passed through the KIV-7HSB 200. Rather, the black side router 206 provides the routing of the WAN 15 link. The red side router 202 provides the routing information for the network traffic and is contained in the encrypted payload encapsulated by the IP encapsulator 204. This information is passed from red side router 202 to red side router of a receiving device.

The disclosed deployable communication system provides 20 up to two simultaneous voice-over-IP calls along with normal data connectivity. Connectivity between the remote system and the enterprise network is provided by the Inmarsat M4 terminal, through connection to a terrestrial ISDN circuit, or by connection to a network or the Internet. Transmissions between the deployed system and enterprise network are 25 encrypted and fully secure up through the Top Secret level through the use of a KIV-7 bulk encryption device.

The deployable communication system allows for routing of bulk encrypted data, a feature not available in any other deployable communication system employing a KIV-7 encryption device.

30 In the disclosed embodiment, commercial off the shelf (COTS) equipment is integrated at the board level into an outer case

made of high quality plastics. The COTS (i.e., commercially available) equipment includes the Cisco 1751V router **202**, the Cisco 801 router **206**, the Engage Communications IPTube-RS-530 **204**, the KIV-7HSB encryption unit **200**, the tri-volt power supply **212**, the DC power supply **210**, and a DC/AC inverter **208**.

Individual components are preferably integrated in such a manner so as to provide separation between encrypted and non-encrypted data, and to ensure protection of the components. Additionally, the specific integration and configuration of the system allows for 10 operation by simply deploying the M4 terminal and applying power. Ideally, the deployable communication system **112** can be powered by universal AC input or by 12 VDC from a vehicle cigarette lighter.

Data entering the deployable communication system **112** and destined for the enterprise network is routed by the red side router 15 **202** and passed to the encryption unit **200** for encryption. Once encrypted, the data is then passed to the IP encapsulator (e.g., IPTube-RS530) **204**, where it is encapsulated into IP packets and passed to the black side Cisco 801 Ethernet to ISDN router **206**.

This data is then passed out of the ISDN port of the black 20 side router **206**, and on to the direct connection to the Inmarsat M4 Terminal **114**, where it is transmitted to the enterprise network.

The deployable communication system **112** accomplishes two specific functions during transmission.

Firstly, an IPSEC tunnel is established between the black 25 side router **206** and a gateway router at the receiving fixed enterprise. This provides privacy for the overall link. Moreover, and very importantly, it presents a commercial/civilian appearance to the transmitted encrypted signal.

Secondly, another tunnel is established between the 30 deployed IP encapsulator **204** and another IP encapsulator at the fixed

enterprise network (or other remote deployable, secure communications terminal).

With this second tunnel established, bulk encrypted data from a KIV-7 type encryption unit 200, which is normally non-routable, is 5 importantly encapsulated in IP packets and routed to the distant end network.

Data encrypted by the KIV-7HSB encryption module 200 normally requires a dedicated, point-to-point circuit for communications to be successful. This is significant for two reasons.

10 First, through the use of the disclosed deployable communication system bulk encrypted data can be routed, thus making use of generic IP or network connections. Moreover, while the deployable communication system would normally be operated with a direct, one to one connection via the Inmarsat M4 Terminal 114, the process of 15 encapsulating the bulk encrypted data into IP packets, and thus routing of the bulk encrypted data, allows for connecting the system into any network—or directly into the Internet via the Ethernet port made available at the output of the IP encapsulator 204.

Second, the unique signature of the government used Type 20 1 encryption is masked by the two separate tunnels and appears as normal commercially encrypted data, thus providing a level of cover to individual operators.

The deployable communications system preferably includes 25 grounding incorporated into grounded AC Power, and is contained in a single deployable case. The disclosed deployable communication system measured about 17"x12"x5" and weighed about 40 pounds, though other small measurements and light weight systems are within the scope of the present invention.

A universal front end accepts between 86-240VAC and 30 provides 24 volts DC to the on-board batteries and the DC/AC inverter. The inverter conditions the power and provides a stable 110 VAC output

for the network components. In the event of commercial power loss, the on-board batteries are sufficient to support operations for the required minimum of 15 minutes and have been tested to operate in excess of 45 minutes. Operation of all system components in a hot standby mode has 5 been demonstrated in excess of two hours. In the event the internal batteries are depleted prior to commercial power restoration, two external 12 volt car batteries can be jumper together and connected into the module for continued operation. This module is integrated into a custom roll-around case measuring 15"W x 24"L x9"D and weighs about 72 lbs 10 including batteries.

Preferably, expansion capabilities may be implemented to support additional users. Moreover, multiple connectivity may be provided by including flexible connection methods and speeds for voice, video and data services, including: a VSAT terminal, an ISDN terminal, an Inmarsat 15 terminal, a conventional dial-up modem, and operate in either a secure or non-secure communications mode.

A single case deployable communications system in accordance with the principles of the present invention has particular application with the US military, federal, local and state agencies, disaster 20 recovery agencies, public safety associations, news channels, and commercial enterprises, to name a few.

The disclosed deployable communication system preferably allows for operation "out of the box", meaning the only component requiring removal is the M4 terminal. Moreover, the deployable 25 communication system is preferably of a size and weight so as to be capable of transport on commercial aircraft as checked baggage.

The term 'encryption' as used herein and in the appended claims relates to a military grade disguising of data in a way intended for proper decryption only by an authorized receiving device.

30 The present invention is disclosed and described with respect to a KIV-7 encryption unit. The principles of IP encapsulation of

encrypted data relate equally well to any type military grade encryption unit, e.g., a KIV-21.

While the invention has been described with reference to the exemplary embodiments thereof, those skilled in the art will be able to 5 make various modifications to the described embodiments of the invention without departing from the true spirit and scope of the invention.